Finite Fields and Their Applications 45 (2017) 43–52

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Further results on permutation trinomials over finite fields with even characteristic

Zhengbang Zha [a,c,*], Lei Hu [b,d], Shuqin Fan [c]

[a] *School of Mathematical Sciences, Luoyang Normal University, Luoyang 471022, China*
[b] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[c] *State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China*
[d] *Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing 100048, China*

A R T I C L E   I N F O

Article history:
Received 24 July 2016
Received in revised form 2 October 2016
Accepted 15 November 2016
Available online xxxx
Communicated by Xiang-dong Hou

MSC:
05A05
11T06
11T55

Keywords:
Finite field
Permutation polynomial
Trace function

A B S T R A C T

Permutation trinomials of the form $x^r h(x^{2^m-1})$ over $\mathbb{F}_{2^{2m}}$ are investigated in this paper, which is a further study on a recent work of Gupta and Sharma. Based on some bijections over the unit circle of $\mathbb{F}_{2^{2m}}$ with order 2^m+1, the two conjectures proposed by Gupta and Sharma are confirmed and several new permutation trinomials are presented.

* Corresponding author.
E-mail addresses: zhazhengbang@163.com (Z. Zha), hu@is.ac.cn (L. Hu), shuqinfan78@163.com (S. Fan).

http://dx.doi.org/10.1016/j.ffa.2016.11.011

1. Introduction

Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements, where p is a prime and n is a positive integer. A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) over $\mathbb{F}_q$ if it induces a bijection on $\mathbb{F}_q$. PPs are an interesting subject of mathematics and engineering, and we refer the reader to [10,14] for more details of the recent advances and contributions to the area.

The existence result of PPs with the form $x^r f(x^{(q-1)/d})$ can be found in [16], where r and d are positive integers with $d \mid (q-1)$. Lee and Park [11] further characterized some trinomial permutations over $\mathbb{F}_q$ in the case of $d = 3$. In [4], Ding et al. obtained several new classes of permutation trinomials by a multivariate approach. Hou [9] determined the permutation behavior of trinomials $ax + bx^q + x^{2q-1} \in \mathbb{F}_{q^2}[x]$ over $\mathbb{F}_{q^2}$. Recently, Gupta and Sharma [7] presented four new classes of trinomial permutations of the form $x^r h(x^{2^m-1})$ over $\mathbb{F}_{2^{2m}}$ and proposed two conjectures about permutation trinomials. Permutation trinomials have simple algebraic form and important applications in various areas such as finite geometry [2,3], combinatorial design [5] and cryptography [6,8]. The recent progress on permutation trinomials can be seen in [12,14] and the references therein.

In this paper, we continue the work of [7] and study permutation trinomials of the form $x^r h(x^{2^m-1})$ over $\mathbb{F}_{2^{2m}}$. By constructing bijections over the unit circle of $\mathbb{F}_{2^{2m}}$ with order $2^m + 1$, we present six new classes of permutation trinomials, which confirm the two conjectures proposed by Gupta and Sharma. Moreover, we describe a relationship between two families of permutation polynomials over $\mathbb{F}_{2^{2m}}$.

2. Preliminaries

Throughout this paper, we always let d, r, m, q be positive integers with $q = 2^{2m}$ and $d|(q-1)$. Let ω be a primitive cubic root of unity in the algebraic closure of $\mathbb{F}_q$ and denote the set of d-th roots of unity by μ_d. For each element x in the finite field $\mathbb{F}_q$, we denote x^{2^m} by $\overline{x}$ in analogy with the usual complex conjugation. Obviously, $x + \overline{x} \in \mathbb{F}_{2^m}$ and $x\overline{x} \in \mathbb{F}_{2^m}$. Define the unit circle of $\mathbb{F}_q$ by the set

$$\mu_{2^m+1} = \{x \in \mathbb{F}_q : x^{2^m+1} = x\overline{x} = 1\}.$$

The trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is defined by

$$\mathrm{Tr}_1^m(x) = x + x^2 + \cdots + x^{2^{m-1}}.$$

Gupta and Sharma in [7] presented two conjectures about permutation trinomials as follows.

Conjecture 1. [7] *The polynomial $f(x) = x^5 + x^{3\cdot 2^m+2} + x^{4\cdot 2^m+1} \in \mathbb{F}_{2^{2m}}[x]$ is a permutation trinomial over $\mathbb{F}_{2^{2m}}$ if and only if $m \equiv 2 \pmod 4$.*